Page 12, after the last line, insert the following:

--I claim:--

IN THE CLAIMS

Please substitute amended claims 1-15 as presented below for the same-numbered claims that were pending prior to the filing of this paper. A marked-up version of the amended claims is attached.

1. (Amended) A method for authenticating a portable object including information processing means and information storage means, the information storage means containing at least one code defining operation steps capable of being executed by the portable object, as well as a one-way function, comprising sending the portable object an order for executing a calculation of a result by applying to said one-way function at least part of said code and using said result to decide whether or not the portable object is authentic.

2. (Amended) A method according to claim 1, wherein said result enters into the implementation of a predetermined operation, said operation being performed successfully only when the portable object is authentic.

3. (Amended) A method according to claim 2, wherein said predetermined operation comprises a decryption operation, said result making it possible to produce an associated decryption key.

4. (Amended) A method according to claim 1, wherein said part of said code used in the calculation, comprises a machine code.

5. (Amended) A method according to claim 1, wherein the portable object contains a real code defining operations designed to be executed by the portable object, and a dummy code defining operations not designed to be executed by the portable object, said code used in the calculation of a result comprising a dummy code.

6. (Amended) A method according to claim 1, further comprising repeatedly sending said order to the portable object during its life, prior to execution by the portable object of said operation steps.

7. (Amended) A method according to claim 1, wherein said code used in the calculation is defined by a start address and an end address in the information storage means, and further including the step of sending said start and end addresses to the portable object.

8. (Amended) A method according to claim 1, wherein said code comprises a set of binary words, said code used in the calculation being defined by a subset of said binary words comprising binary words distributed in the information storage means at a determined pitch, said pitch being sent to the portable object.

9. (Amended) A method for having a portable object execute a sensitive operation, the portable object comprising information processing means and information storage means, comprising: storing in the information storage means at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and sending the portable object an order so that the portable object executes a calculation of a result by applying to said one-way function at least part of said code, said result entering into the implementation of said sensitive operation, said operation being performed successfully only when the portable object is authentic.

10. (Amended) A method according to claim 9, wherein the code part used in the calculation comprises a machine code.

11. (Amended) A method according to claim 9, wherein the portable object contains a real code defining operations designed to be executed by the portable object, and a dummy code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code.

12. (Amended) A portable object, comprising: information processing means, information storage means, the information storage means containing at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and means for executing a calculation of a result by applying to said one-way function at least part of said code.

13. (Amended) A portable object according to claim 12, wherein said code part used in the calculation comprises a machine code.

14. (Amended) A device comprising: information processing means, information storage means, said information processing means designed to communicate with a portable object in order to authenticate the portable object, the portable object comprising: information processing means, information storage means, the information storage means of the portable object containing at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and means for sending the portable object an order so that

the portable object executes a calculation of a result by applying to said one-way function at least part of said code of the portable object.

15. (Amended) A device according to claim 14, wherein said code part used in the calculation comprises a machine code.